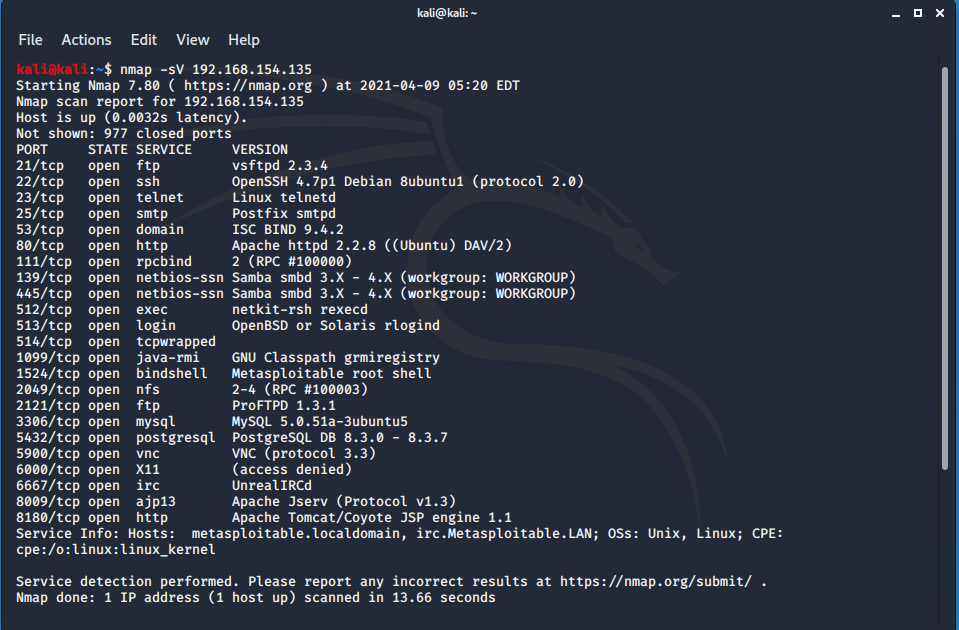
IT18107692 – N. K Madanayake

IT – Weekend

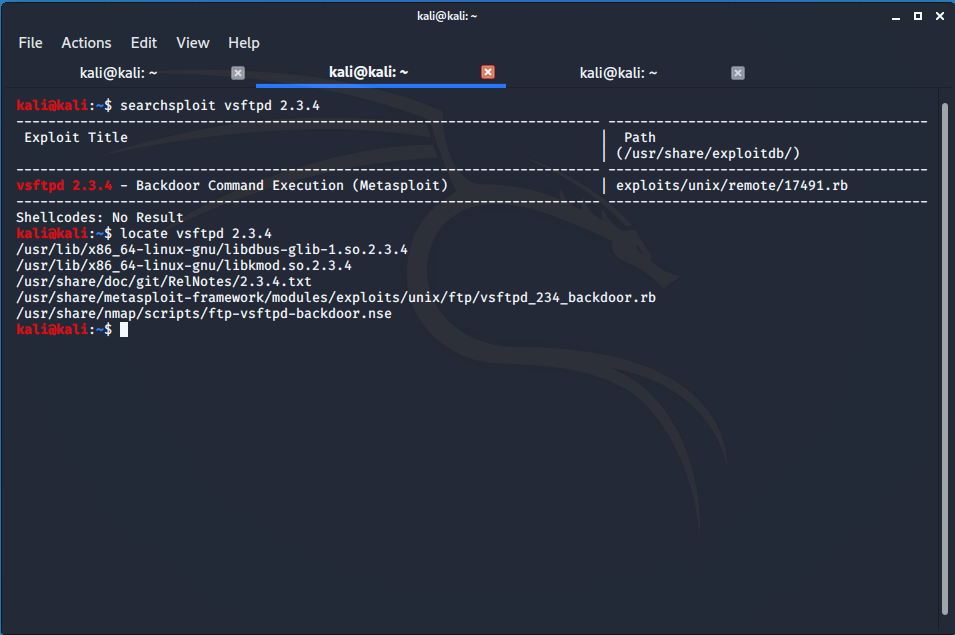
Exploit Vulnerabilities in Metasploit 2

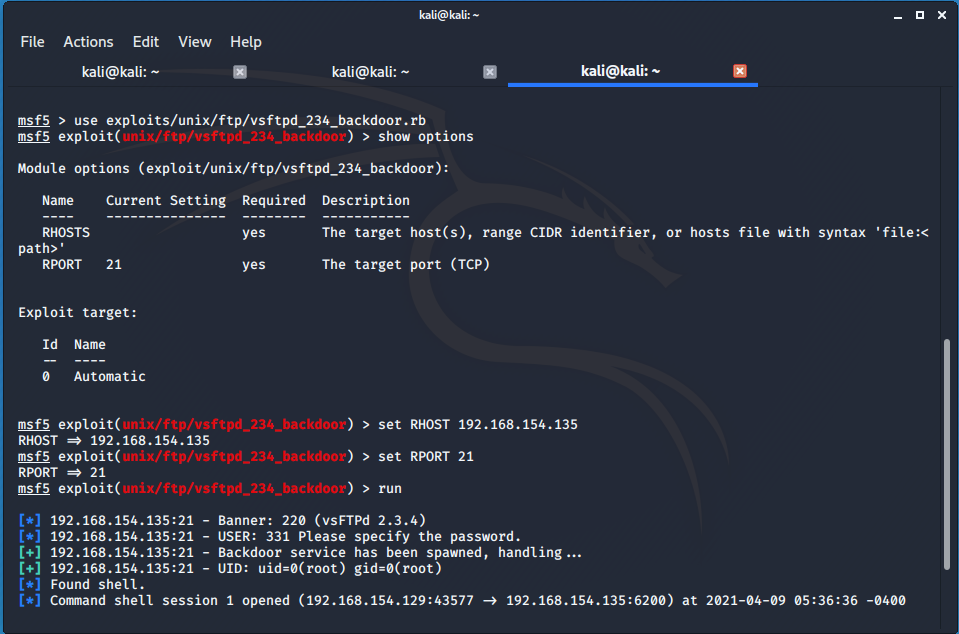
# **Nmap -using nmap to identify services on the vulnerable machines.**

When we scan metasploitable 2 machine using nmap, we have a few common ports like SSH and FTP and we have enumerated their service version number, which means we can now perform some vulnerability analysis on each of these services.



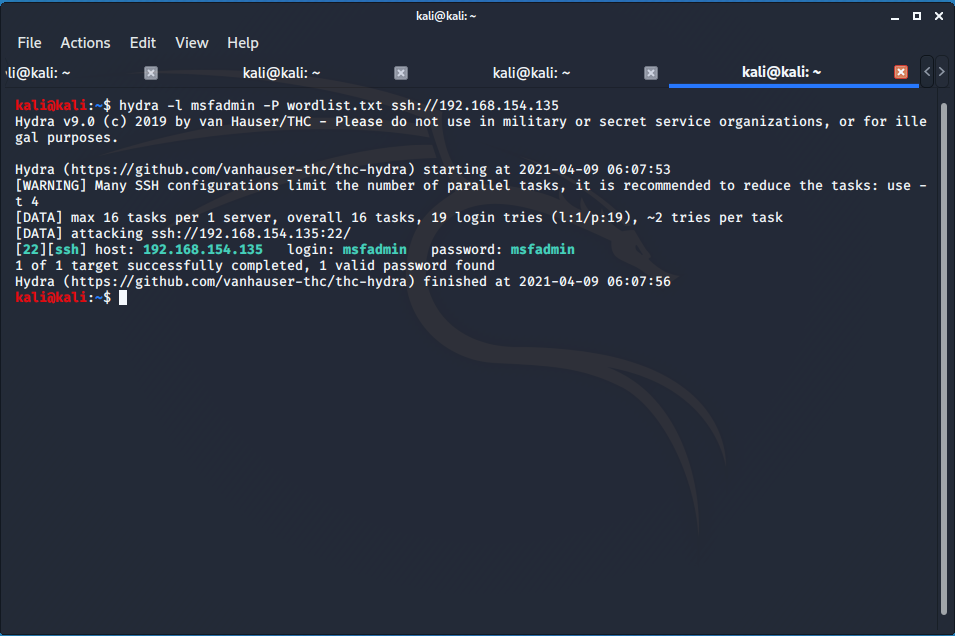
We can use **searhsploit** command to check weather those versions of services has vulnerabilities and relevant exploits to exploit them. In here we found **vsftpd 2.3.4** is vulnerable and we found suitable exploit by using **searchsploit** command.



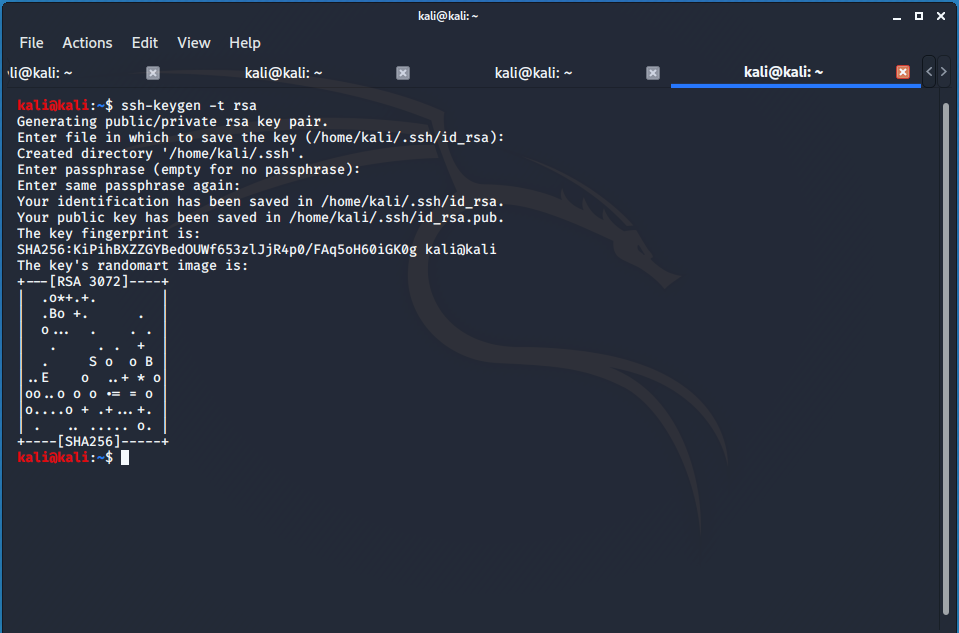
Then we can start metasploit framework using **msfconsole** command. We locate the exploit earlier by using **locate** command and now we can use the exploit using **use** command. After use the exploit we can see options using **show options** command. Then we can set remote host and remote port. After that we can exploit using **run** command. It will create remote session to target machine.

# **Brute-Force SSH Attack**

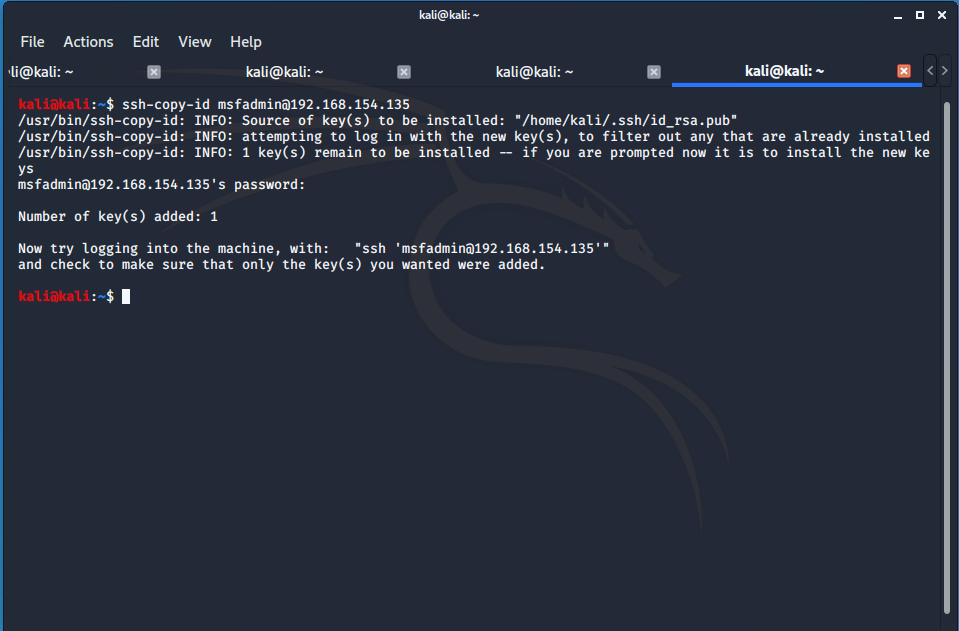
After performing some basic vulnerability analysis with **searchsploit**, we discover no vulnerability on the current version of OpenSSH, however the other attack vector we can target or use, is the brute force attack.

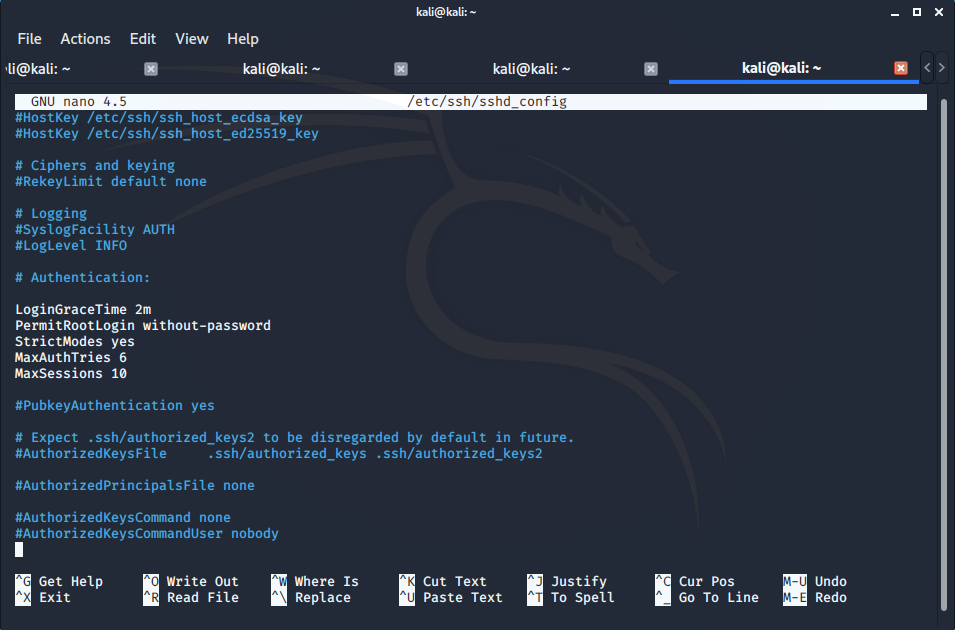
We can make password list and brute force it using the tool called hydra. We can find unknown username or password of the target machine by this method.

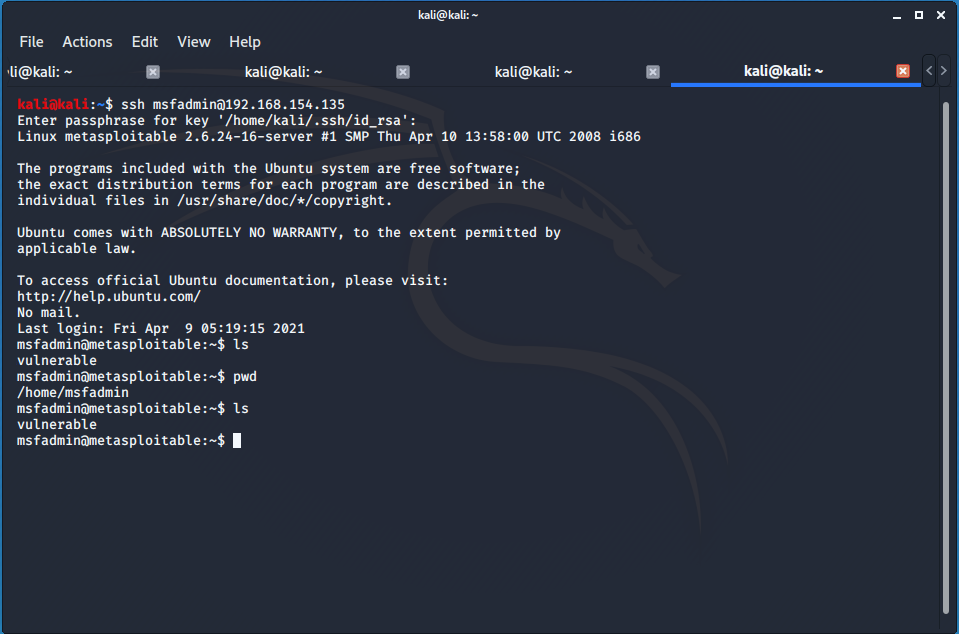
# **Setting up SSH keys**

We are able to get the SSH password for the user msfadmin very easily, this shows us the importance of securing SSH correctly. The remedy for this problem is use SSH keys rather than passwords. In this method first we need to generate key pair on client computer.

We then need to enter our passphrase, this is not mandatory but it is highly recommended, it adds an extra layer of security to our SSH keys, as unauthorized individuals will not be able to use the SSH key to authenticate without the password.

Then we can copy the public key to the server

Now that we have set up our authentication using SSH keys, we can now disable SSH password authentication, therefore nullifying brute force attacks on the SSH port. To do this we need to modify the SSH configuration file on the server located in **/etc/ssh/sshd\_config**. To make sure users can only connect to the server via their SSH key, modify the **PermitRootLogin** and set the value **towithout-password**. Once done, save and close the file. Then restart SSH service to add new modifications.

After that you can login using SSH keys